

# New Classes of Permutation Binomials and Permutation Trinomials over Finite Fields

Kangquan Li, Longjiang Qu, and Xi Chen

## Abstract

Permutation polynomials over finite fields play important roles in finite fields theory. They also have wide applications in many areas of science and engineering such as coding theory, cryptography, combinational design, communication theory and so on. Permutation binomials and trinomials attract people's interest due to their simple algebraic form and additional extraordinary properties. In this paper, several new classes of permutation binomials and permutation trinomials are constructed. Some of these permutation polynomials are generalizations of known ones.

## Index Terms

Finite Field, Permutation Polynomial, Permutation Binomial, Permutation Trinomial.

## 1. INTRODUCTION

A polynomial  $f \in \mathbb{F}_q[x]$  is called a permutation polynomial of  $\mathbb{F}_q$  if the associated polynomial function  $f : c \rightarrow f(c)$  from  $\mathbb{F}_q$  into  $\mathbb{F}_q$  is a permutation of  $\mathbb{F}_q$ . Permutation polynomials over finite fields play important roles in finite fields theory. They also have wide applications in coding theory, cryptography, combinational design, communication theory. The study of permutation polynomial can date back to Hermite [12] and Dickson [7]. There are numerous books and survey papers on the subject covering different periods in the development of this active area [6, Ch.18], [14], [22, Ch.7], [23, Ch.8], [15], while the survey by X. Hou [15] in 2015 is the most recent one.

Permutation binomials and trinomials attract people's interest due to their simple algebraic form and additional extraordinary properties. For instances, a certain permutation trinomial of  $\mathbb{F}_{2^{2m+1}}$  was a major ingredient in the proof of the Welch conjecture [10]. The discovery of other class of permutation trinomials by Ball and Zieve [1] provides a way to prove the construction of the Ree-Tits symplectic spreads of  $\mathbf{PG}(3, q)$ . For more relevant progresses, readers can consult a paper [14] presented by X.Hou, which conducted a recent survey on permutation binomials and trinomials in 2013.

The authors are with the College of Science, National University of Defense Technology, ChangSha, 410073, China, email: 940672099@qq.com, ljqu\_happy@hotmail.com, 1138470214@qq.com. The research of this paper is supported by the NSFC of China under Grant 61272484, the National Basic Research Program of China(Grant No. 2013CB338002), the Basic Research Fund of National University of Defense Technology (No. CJ 13-02-01) and the Program for New Century Excellent Talents in University (NCET).

Although quite a few permutation binomials and permutation trinomials have been found, however, an explicit and unify characterization of them is still missing and seems to be elusive today. Therefore, it is both interesting and important to find more explicit classes of them and try to find the hidden reason for their permutation property. In this paper, we present several new classes of permutation binomials over finite fields with even extensions and permutation trinomials over finite fields with even characteristics. Therefore we will review the known permutation binomials over  $\mathbb{F}_{q^2}$  and permutation trinomials over  $\mathbb{F}_{2^m}$  in Section 3-A and Section 4-A, respectively for the convenience of the reader. For other classes of permutation binomials or permutation trinomials, please refer to [14].

In Section 2, we introduce the definition of the multiplicative equivalence of permutation polynomials and some lemmas. In Section 3, we provide new classes of permutation binomials through the Hermite's criterion [12] and considering the number of solutions of special equations. In Section 4, we give five new classes of permutation trinomials. Section 5 is the conclusion. In the paper,  $\text{Tr}_k(x)$  is treated as the absolute trace function on  $\mathbb{F}_{2^k}$ . The algebraic closure of  $\mathbb{F}_q$  is denoted by  $\bar{\mathbb{F}}_q$ . For integer  $d > 0$ ,  $\mu_d = \{x \in \bar{\mathbb{F}}_q : x^d = 1\}$ . Others symbols follow the standard notation of finite fields.

## 2. PREPARATION

Let  $f$  and  $g$  be two polynomials in  $\mathbb{F}_q[x]$  satisfying that  $f(x) = g(x^d)$ , where  $1 \leq d \leq q-1$  is an integer such that  $\gcd(d, q-1) = 1$ . Then the number of the terms of  $f$  is equal to that of  $g$ , and  $f$  is a permutation polynomial if and only if so is  $g$ . Particularly,  $f$  is a permutation binomial resp. permutation trinomial if and only if so is  $g$ . Hence we introduce the following definition of multiplicative equivalence.

**Definition 2.1.** *Two permutation polynomials  $f(x)$  and  $g(x)$  in  $\mathbb{F}_q[x]$  are called multiplicative equivalent if there exists an integer  $1 \leq d \leq q-1$  such that  $\gcd(d, q-1) = 1$  and  $f(x) = g(x^d)$ .*

It should be noted that in [15] and many references before, two permutation polynomial  $f$  and  $g$  of  $\mathbb{F}_q$  called equivalent if  $f(x) = cg(ax+b) + d$ , where  $a, c \in \mathbb{F}_q^*$ ,  $b, d \in \mathbb{F}_q$ . In our opinion, this type of equivalence can be called linear equivalence.

The following lemmas will be useful in our future discussion. The first one is a corollary following directly from [27, Lemma 2.1].

**Lemma 2.2.** *Let  $f(x) = x^{r_0}(x^{(q-1)/d} + a) \in \mathbb{F}_q[x]$ , where  $d \mid q-1$ ,  $a \in \mathbb{F}_q^*$ . If  $f(x)$  is a permutation polynomial over  $\mathbb{F}_q$  and  $\gcd(r_0 + d, (q-1)/d) = 1$ , then  $g(x) = x^{r_0+d}(x^{(q-1)/d} + a)$  is also a permutation polynomial over  $\mathbb{F}_q$ .*

**Lemma 2.3.** [22] (Hermite's Criterion) *Let  $\mathbb{F}_q$  be of characteristic  $p$ . Then  $f \in \mathbb{F}_q[x]$  is a permutation polynomial of  $\mathbb{F}_q$  if and only if the following two conditions hold:*

- (i)  *$f$  has exactly one root in  $\mathbb{F}_q$ ;*
- (ii) *for each integer  $t$  with  $1 \leq t \leq q-2$  and  $t \not\equiv 0 \pmod{p}$ , the reduction of  $f(x)^t \pmod{x^q - x}$  has degree  $\leq q-2$ .*

**Lemma 2.4.** (Lucas formula) *Let  $n, i$  be positive integers and  $p$  be a prime. Assume  $n = a_m p^m + \dots + a_1 p + a_0$  and  $i = b_m p^m + \dots + b_1 p + b_0$ . Then  $\binom{n}{i} \equiv \binom{a_m}{b_m} \binom{a_{m-1}}{b_{m-1}} \dots \binom{a_0}{b_0} \pmod{p}$ .*

**Lemma 2.5.** *Let  $q = 2^k$  and  $k > 0$  be an integer. Then  $f(x) = x + x^2 + x^4$  is a permutation polynomial over  $\mathbb{F}_q$  if and only if  $k \not\equiv 0 \pmod{3}$ .*

*Proof:* This lemma can be easily proved. We omit it here. ■

**Lemma 2.6.** [2] *Let  $a \in \mathbb{F}_{2^k}^*$ . Then the cubic equation  $x^3 + x = a$  has a unique solution in  $\mathbb{F}_{2^k}$  if and only if  $\text{Tr}_k(a^{-1}) \neq \text{Tr}_k(1)$ .*

### 3. PERMUTATION BINOMIALS

Given  $f(x) = x^m + ax^n \in \mathbb{F}_q[x]$ , where  $0 < n < m < q$  and  $a \in \mathbb{F}_q^*$ , there exist integers  $r, t, d > 0$  with  $\gcd(t, q-1) = 1$  and  $d \mid q-1$  such that  $f(x^t) \equiv x^r(x^{(q-1)/d} + a) \pmod{x^q - x}$  [15]. Therefore, w.l.o.g, we only consider permutation binomials with the form  $x^r(x^{(q-1)/d} + a)$ . Inspired by Hou and Lappano [13], in this section, we consider permutation binomials over finite fields with even extensions, that is, over  $\mathbb{F}_{q^2}$ .

#### A. Known permutation binomials over $\mathbb{F}_{q^2}$

First, we review the known permutation binomials over finite fields with even extensions.

**Theorem 3.1.** [27] *Let  $r, d > 0$  be integers such that  $d \mid q^2 - 1$  and  $a \in \mathbb{F}_{q^2}^*$ . Further assume that  $\eta + \frac{a}{\eta} \in \mu_{(q^2-1)/d}$  for all  $\eta \in \mu_{2d}$ . Then  $x^r(x^{(q^2-1)/d} + a)$  is a permutation polynomial of  $\mathbb{F}_{q^2}$  if and only if  $-a \notin \mu_d$ ,  $\gcd(2d, 2r + (q^2 - 1)/d) \leq 2$ .*

**Theorem 3.2.** [28] *Let  $r$  and  $d$  be positive integers, and let  $\beta \in \mathbb{F}_{q^2}$  be such that  $\beta^{q+1} = 1$ . Then  $x^{r+d(q-1)} + \beta^{-1}x^r$  is a permutation polynomial of  $\mathbb{F}_{q^2}$  if and only if all of the following hold:*

- (i)  $\gcd(r, q-1) = 1$ .
- (ii)  $\gcd(r-d, q+1) = 1$ .
- (iii)  $(-\beta)^{(q+1)/\gcd(q+1, d)} \neq 1$ .

**Theorem 3.3.** [13] *Let  $f = ax + x^{3q-2} \in \mathbb{F}_{q^2}[x]$ , where  $a \in \mathbb{F}_{q^2}^*$ . Then  $f$  is a permutation polynomial of  $\mathbb{F}_{q^2}$  if one of the following occurs.*

- (i)  $q = 2^{2k+1}$  and  $a^{\frac{q+1}{3}}$  is a primitive 3rd root of unity.
- (ii)  $q = 5$  and  $a^2$  is a root of  $(x+1)(x+2)(x-2)(x^2-x+1)$ .
- (iii)  $q = 2^3$  and  $a^3$  is a root of  $x^3 + x + 1$ .
- (iv)  $q = 11$  and  $a^4$  is a root of  $(x-5)(x+2)(x^2-x+1)$ .
- (v)  $q = 17$  and  $a^6 = 4, 5$ .
- (vi)  $q = 23$  and  $a^8 = -1$ .
- (vii)  $q = 29$  and  $a^{10} = -3$ .

**Theorem 3.4.** [19] Let  $f = ax + x^{5q-4} \in \mathbb{F}_{q^2}[x]$ , where  $a \in \mathbb{F}_{q^2}^*$ . Then  $f$  is a permutation polynomial of  $\mathbb{F}_{q^2}$  if one of the following occurs.

- (i)  $q = 2^{4k+2}$  and  $a^{\frac{q+1}{5}}$  is a primitive 5th root of unity.
- (ii)  $q = 3^2$  and  $a^2$  is a root of  $(x+1)(x^2+1)(x^2+x+2)(x^2+2x+2)(x^4+x^2+x+1)(x^4+x^3+x^2+1)(x^4+2x^3+x^2+2x+1)$ .
- (iii)  $q = 19$  and  $a^4$  is a root of  $(x+1)(x+2)(x+3)(x+4)(x+5)(x+9)(x+10)(x+13)(x+17)(x^2+3x+16)(x^2+4x+1)(x^2+18x+6)$ .
- (iv)  $q = 29$  and  $a^6 \in \{15, 18, 22, 23\}$ .
- (v)  $q = 7^2$  and  $a^{10}$  is a root of  $x^2+4x+1$ .
- (vi)  $q = 59$  and  $a^{12}$  is a root of  $(x^2+x+1)(x^3+x+1)$ .
- (vii)  $q = 2^6$  and  $a^{13}$  is a root of  $(x^2+x+1)(x^3+x+1)$ .

### B. New classes of permutation binomials

**Theorem 3.5.** Let  $f(x) = x(x^{q+1} + a) \in \mathbb{F}_{q^2}[x]$ . Then  $f(x)$  is a permutation binomial over  $\mathbb{F}_{q^2}$  if and only if  $q \not\equiv 1 \pmod{3}$  and  $a^{2(q-1)} - a^{q-1} + 1 = 0$ .

*Proof:* First of all, we show that when  $q \equiv 1 \pmod{3}$ ,  $f(x)$  is not a permutation polynomial over  $\mathbb{F}_{q^2}$ .

Let  $0 \leq \alpha, \beta \leq q-1$  with  $(\alpha, \beta) \neq (0, 0)$ . Then we have

$$\begin{aligned} \sum_{x \in \mathbb{F}_{q^2}} f(x)^{\alpha+q\beta} &= \sum_{x \in \mathbb{F}_{q^2}} (ax + x^{q+2})^\alpha (a^q x^q + x^{1+2q})^\beta \\ &= \sum_{x \in \mathbb{F}_{q^2}} \sum_{0 \leq i \leq \alpha, 0 \leq j \leq \beta} \binom{\alpha}{i} a^{\alpha-i} x^{\alpha-i} x^{(q+2)i} \binom{\beta}{j} a^{q(\beta-j)} x^{q(\beta-j)} x^{(1+2q)j} \\ &= a^{\alpha+q\beta} \sum_{0 \leq i \leq \alpha, 0 \leq j \leq \beta} \binom{\alpha}{i} \binom{\beta}{j} a^{-i-qj} \sum_{x \in \mathbb{F}_{q^2}^*} x^{\alpha+q\beta+(1+q)(i+j)}. \end{aligned}$$

The inner sum is 0 unless  $\alpha + q\beta + (1+q)(i+j) \equiv 0 \pmod{q^2-1}$ , which can happen only if  $\alpha + \beta q \equiv 0 \pmod{q+1}$ , or equivalently,  $\alpha = \beta$ . Then we have

$$\sum_{x \in \mathbb{F}_{q^2}^*} f(x)^{\alpha+q\beta} = -a^{(1+q)\alpha} \sum_{\substack{\alpha+i+j \equiv 0 \pmod{q-1}, \\ 0 \leq i, j \leq \alpha}} \binom{\alpha}{i} \binom{\alpha}{j} a^{-i-qj}.$$

Let  $\alpha = \frac{q-1}{3}$ . Then

$$\sum_{x \in \mathbb{F}_{q^2}} f(x)^{\alpha+q\alpha} = -a^{(q+1)\alpha} a^{-\alpha-\alpha q} = -1 \neq 0.$$

Hence, in the case,  $f(x)$  is not a permutation polynomial over  $\mathbb{F}_{q^2}$ .

In the following, we show that when  $q \not\equiv 1 \pmod{3}$ ,  $f(x)$  is a permutation polynomial over  $\mathbb{F}_{q^2}$  if and only if  $a^{2(q-1)} - a^{q-1} + 1 = 0$ .

First, it is easy to prove that zero is the only root of  $f(x) = 0$  in  $\mathbb{F}_q$  if and only if  $a^{q-1} \neq 1$ .

Next we prove that  $f(x) = c$  has at most one solution in  $\mathbb{F}_{q^2}$  for any  $c \in \mathbb{F}_{q^2}^*$  if and only if  $a^{2(q-1)} - a^{q-1} + 1 = 0$ . It is clear that 0 is not a solution. Therefore we consider the following equation

$$x^{q+1} + a = \frac{c}{x}. \quad (1)$$

Let  $u = \frac{c}{x} - a = x^{q+1}$ . Then  $u \in \mathbb{F}_q^*$  and  $x = \frac{c}{a+u}$ . Plugging it into (1), one have

$$\left( \frac{c}{a+u} \right)^{q+1} = u.$$

After simplifying and rearranging the terms, we get

$$u^3 + (a^q + a)u^2 + a^{q+1}u = c^{q+1}. \quad (2)$$

Let  $a_2 = a^q + a$ ,  $a_1 = a^{q+1}$ ,  $a_0 = -c^{q+1}$ . Then  $f(x) = c$  has at most one solution in  $\mathbb{F}_{q^2}$  if and only if  $g(u) = u^3 + a_2u^2 + a_1u$  is a permutation polynomial over  $\mathbb{F}_q$ . In the following, we will use the table of normalized permutation polynomials over  $\mathbb{F}_q$  (Table 7.1 in [22]). Recall that a polynomial  $\phi$  is called in normalized form if  $\phi$  is monic,  $\phi(0) = 0$ , and when the degree  $n$  of  $\phi$  is not divisible by the characteristic of  $\mathbb{F}_q$ , the coefficient of  $x^{n-1}$  is 0. The rest of the proof is split into two cases.

Case 1:  $q \equiv 2 \pmod{3}$ .

Let  $u = v - \frac{a_2}{3}$ . Plugging it into (2), we get

$$v^3 + \mu_1v + \mu_2 = 0.$$

where  $\mu_1 = -\frac{1}{3}a_2^2 + a_1$ ,  $\mu_2 = \frac{2}{27}a_2^3 - \frac{1}{3}a_1a_2 + a_0$ . Then  $\mu_1, \mu_2 \in \mathbb{F}_q$ .

As  $f(x) = c$  has at most one solution in  $\mathbb{F}_{q^2}$  if and only if  $h(v) = v^3 + \mu_1v$  is a permutation polynomial over  $\mathbb{F}_q$ , which holds if and only if  $\mu_1 = 0$  by [22, Table 7.1]. Recalling that  $\mu_1 = -\frac{1}{3}a^2(a^{2(q-1)} - a^{q-1} + 1)$ , we come to the conclusion that  $f(x) = c$  has at most one solution in  $\mathbb{F}_{q^2}$  if and only if  $a^{2(q-1)} - a^{q-1} + 1 = 0$ .

Case 2:  $q \equiv 0 \pmod{3}$ .

In this case,  $g(u) = u^3 + a_2u^2 + a_1u$  is already a normalized polynomial. According to [22, Table 7.1],  $x^3 - ax$  ( $a$  is not a square) and  $x^3$  are the two normalized permutation polynomials over  $\mathbb{F}_q$  with degree three. On one hand, if  $g$  permutes  $\mathbb{F}_q$ , then we have  $a_2 = 0$ . Thus  $a^{q-1} + 1 = 0$ , or equivalently,  $0 = (a^{q-1} + 1)^2 = a^{2(q-1)} - a^{q-1} + 1$ . On the other hand, if  $a^{q-1} + 1 = 0$ , then  $g(u) = u^3 - a^2u$ . Clearly,  $a^2$  is a non-square in  $\mathbb{F}_q$  since  $a \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ . Hence  $g(u)$  permutes  $\mathbb{F}_q$ .

We finish the proof. ■

We briefly discuss the multiplicative inequivalence of the new permutation binomial in Theorem 3.5 with known ones. Due to the special and specific conditions in Theorem 3.5 and those in the last subsection, the permutation binomial  $f(x)$  of Theorem 3.5 is not multiplicative equivalent to any known permutation binomial. According to Lemma 2.2, if  $\gcd(1 + l(q-1), q+1) = 1$ , where  $l$  is an integer, the polynomial  $x^{1+l(q-1)}(x^{q+1} + a)$  is also a permutation binomial over  $\mathbb{F}_{q^2}$ .

Theorem 3.5 considers permutation binomials of  $\mathbb{F}_{q^2}$  with the form  $x(x^{q+1}+a)$ . Next, we consider another permutation binomial with the form  $x^r(x^{q-1}+a)$ , where  $r \in [1, q+1]$ .

**Theorem 3.6.** *Let  $f(x) = x^r(x^{q-1}+a) \in \mathbb{F}_{q^2}[x]$ ,  $r \in [1, q+1]$ . Then  $f(x)$  is a permutation binomial over  $\mathbb{F}_{q^2}$  if and only if  $r = 1$  and  $a^{q+1} \neq 1$ .*

*Proof:* First, it is clear that  $f(x) = x^r(x^{q-1}+a)$  has only one root in  $\mathbb{F}_{q^2}$  if and only if  $a^{q+1} \neq 1$ . Next, let  $0 \leq \alpha, \beta \leq q-1$  with  $(\alpha, \beta) \neq (0, 0), (q-1, q-1)$ . We have

$$\begin{aligned} \sum_{x \in \mathbb{F}_{q^2}} f(x)^{\alpha+\beta q} &= \sum_{x \in \mathbb{F}_{q^2}} x^{r(\alpha+\beta q)} (x^{q-1}+a)^{(\alpha+\beta q)} \\ &= \sum_{x \in \mathbb{F}_{q^2}^*} x^{r(\alpha+\beta q)} (x^{q-1}+a)^\alpha (x^{1-q}+a^q)^\beta \\ &= \sum_{x \in \mathbb{F}_{q^2}^*} x^{r(\alpha+\beta q)} \sum_{i=0}^{\alpha} \binom{\alpha}{i} x^{i(q-1)} a^{\alpha-i} \sum_{j=0}^{\beta} \binom{\beta}{j} x^{j(1-q)} (a^q)^{\beta-j} \\ &= a^{\alpha+\beta q} \sum_{0 \leq i \leq \alpha, 0 \leq j \leq \beta} \binom{\alpha}{i} \binom{\beta}{j} a^{-i-qj} \sum_{x \in \mathbb{F}_{q^2}^*} x^{r(\alpha+\beta q)+(i-j)(q-1)}. \end{aligned}$$

The inner sum is 0 unless  $r(\alpha+\beta q) + (i-j)(q-1) \equiv 0 \pmod{q^2-1}$ , which can happen only if  $\alpha+\beta q \equiv 0 \pmod{q-1}$ , or equivalently,  $\alpha+\beta = q-1$ . Let  $\beta = q-1-\alpha$ . Then we have

$$\begin{aligned} \sum_{x \in \mathbb{F}_{q^2}} f(x)^{\alpha+(q-1-\alpha)q} &= a^{(\alpha+1)(1-q)} \sum_{0 \leq i \leq \alpha, 0 \leq j \leq q-1-\alpha} \binom{\alpha}{i} \binom{q-1-\alpha}{j} a^{-i-qj} \sum_{x \in \mathbb{F}_{q^2}^*} x^{(q-1)(-r(\alpha+1)+i-j)} \\ &= -a^{(\alpha+1)(1-q)} \sum_{-r(\alpha+1)+i-j \equiv 0 \pmod{q+1}} \binom{\alpha}{i} \binom{q-1-\alpha}{j} a^{-i-qj}. \end{aligned}$$

As  $i$  runs over the interval  $[0, \alpha]$  and  $j$  over the interval  $[0, q-1-\alpha]$ ,  $-r(\alpha+1)+i-j \in S_{\alpha,r}$ , where

$$S_{\alpha,r} = [-r(\alpha+1) - (q-1-\alpha), -r(\alpha+1) + \alpha].$$

If  $r = 1$ , then  $S_{\alpha,r} = [-q, -1]$ , and the equation  $-(\alpha+1)+i-j \equiv 0 \pmod{q+1}$  has no solution. Therefore,  $\sum_{x \in \mathbb{F}_{q^2}} f(x)^{\alpha+(q-1-\alpha)q} = 0$ . Hence,  $f(x)$  is a permutation polynomial over  $\mathbb{F}_{q^2}$ .

If  $r \in [2, q+1]$ , let  $\alpha = 0$ . Then  $S_{0,r} = [-r-q+1, -r]$ . In the case, the only multiple of  $q+1$  in  $S_{0,r}$  is  $-(q+1)$ . Therefore, we have

$$\sum_{x \in \mathbb{F}_{q^2}} f(x)^{(q-1)q} = -a^{(1-q)} \binom{q-1}{q+1-r} a^{-1-q+rq} = - \binom{q-1}{q+1-r} a^{(r-2)q}.$$

It follows from Lucas formula that  $\binom{q-1}{q+1-r} \not\equiv 0 \pmod{p}$  if  $r \in [2, q+1]$ . Therefore,  $\sum_{x \in \mathbb{F}_{q^2}} f(x)^{(q-1)q} \neq 0$ .

Hence, when  $r \in [2, q+1]$ ,  $f(x)$  is not a permutation polynomial over  $\mathbb{F}_{q^2}$ .

The proof is finished. ■

In Theorem 3.6, let  $r = 1$ , then we get  $f(x) = x^r(x^{q-1} + a) = x^q + ax$ , which is a linearized polynomial. Hence Theorem 3.6 does not provide new permutation binomial. However, to the authors' best knowledge, the characterization of the sufficient and necessary condition for the polynomial with this form to be a permutation is new.

#### 4. PERMUTATION TRINOMIALS

##### A. The known permutation trinomials

First, we review the known permutation trinomials over  $\mathbb{F}_{2^m}$ . The results before 2014 were summarized in [9]. We copy their list into the following theorem for the readers' conveniences,

**Theorem 4.1.** 1) Some linearized permutation trinomials described in [22].

- 2)  $x + x^3 + x^5$  over  $\mathbb{F}_{2^m}$ , where  $m$  is odd (the Dickson polynomial of degree 5).
- 3)  $x + x^5 + x^7$  over  $\mathbb{F}_{2^m}$ , where  $m \not\equiv 0 \pmod{3}$  (the Dickson polynomial of degree 7).
- 4)  $x + x^3 + x^{2^{(m+1)/2}+1}$  over  $\mathbb{F}_{2^m}$ , where  $m$  is odd [10].
- 5)  $x^{2^{2k}+1} + (ax)^{2^k+1} + ax^2$  over  $\mathbb{F}_{2^m}$ , where  $m = 3k$  and  $a^{(2^m-1)/(2^k-1)} \neq 1$  [3].
- 6)  $x^{3 \cdot 2^{(m+1)/2}+4} + x^{2^{(m+1)/2}+2} + x^{2^{(m+1)/2}}$  over  $\mathbb{F}_{2^m}$ , where  $m$  is odd ([5] or [11, Theorem 4]).
- 7)  $x^{2^{2k}+1} + x^{2^k+1} + vx$  over  $\mathbb{F}_{2^m}$ , where  $m = 3k$  and  $v \in \mathbb{F}_{2^k}^*$  [25].
- 8) [20] Let  $q \equiv 1 \pmod{3}$  be a prime power. Let  $\alpha$  be a generator of  $\mathbb{F}_q^*$ ,  $s = (q-1)/3$ , and let  $\omega = \alpha^s$ . Define  $f(x) = ax^2 + bx + c \in \mathbb{F}_q[x]$ . Then

$$h(x) := x^r f(x^s)$$

is a permutation polynomial over  $\mathbb{F}_q$  if and only if the following conditions are satisfied:

- a)  $\gcd(r, s) = 1$ ,
- b)  $f(\omega^i) \neq 0$  for  $0 \leq i \leq 2$ ,
- c)  $\log_\alpha(f(1)/f(\omega)) \equiv \log_\alpha(f(\omega)/f(\omega^2)) \not\equiv r \pmod{3}$ .

The following results are new classes of permutation trinomials constructed in [9].

**Theorem 4.2.** [9] Let  $m > 1$  be an odd integer. Then both  $x + x^{2^{(m+1)/2}-1} + x^{2^m-2^{(m+1)/2}+1}$  and  $x + x^3 + x^{2^m-2^{(m+3)/2}+2}$  are permutation polynomials over  $\mathbb{F}_{2^m}$ .

**Theorem 4.3.** [9] Let  $m$  be a positive even integer. Then  $x + x^{2^{(m+2)/2}-1} + x^{2^m-2^{m/2}+1}$  is a permutation polynomial over  $\mathbb{F}_{2^m}$ .

**Theorem 4.4.** [9] Let  $k$  be a positive integer and  $q$  be a prime power with  $q \not\equiv 0 \pmod{3}$ . Let  $m$  be a positive even integer. Then,  $x + x^{kq^{m/2}-(k-1)} + x^{k+1-kq^{m/2}}$  is a permutation polynomial over  $\mathbb{F}_{q^m}$  if and only if one of the following three conditions holds:

- (i)  $m \equiv 0 \pmod{4}$ ;
- (ii)  $q \equiv 1 \pmod{4}$ ;
- (iii)  $m \equiv 2 \pmod{4}$ ,  $q \equiv 2 \pmod{3}$ , and  $\exp_3(q^{m/2} + 1)$ , where  $\exp_3(i)$  denotes the exponent of 3 in the canonical factorization of  $i$ .

Recently, some particular types of permutation trinomials have been determined by Hou. We list these following permutation trinomials in even characteristic.

**Theorem 4.5.** [18] *Let  $f = ax + bx^q + x^{2q-1} \in \mathbb{F}_{q^2}[x]$ , where  $q$  is even. Then  $f$  is a permutation polynomial over  $\mathbb{F}_{q^2}$  if and only if one of the following is satisfied.*

- (i)  $a = b = 0, q = 2^{2k}$ .
- (ii)  $ab \neq 0, a = b^{1-q}, \text{Tr}_{q/2}(b^{-1-q}) = 0$ .
- (iii)  $ab(a - b^{1-q}) \neq 0, \frac{a}{b^2} \in \mathbb{F}_q, \text{Tr}_{q/2}(\frac{a}{b^2}) = 0, b^2 + a^2b^{q-1} + a = 0$ .

**Theorem 4.6.** [16] *Let  $q > 2$  be even and  $f = x + tx^q + x^{2q-1} \in \mathbb{F}_q[x]$ , where  $t \in \mathbb{F}_q^*$ . Then  $f$  is a permutation polynomial of  $\mathbb{F}_{q^2}$  if and only if  $\text{Tr}_{q/2}(\frac{1}{t}) = 0$ .*

#### B. New Classes of Permutation Trinomials

In this subsection, we introduce five new classes of permutation trinomials over  $\mathbb{F}_{2^m}$ . Motivated by [9], we first consider permutation trinomials with trivial coefficients, that is, whose nonzero coefficients are all 1.

**Theorem 4.7.** *Let  $q = 2^{2k}$  and  $k$  be a positive integer. Then  $f(x) = x + x^{2^k} + x^{2^{2k-1}-2^{k-1}+1}$  is a permutation trinomial over  $\mathbb{F}_q$  if and only if  $k \not\equiv 0 \pmod{3}$ .*

*Proof:* First of all, we show that  $x = 0$  is the only solution of  $f(x) = 0$  in  $\mathbb{F}_q$  when  $k \not\equiv 0 \pmod{3}$ . If  $f(x) = 0$ , then either  $x = 0$  or  $1 + x^{2^k-1} + x^{2^{2k-1}-2^{k-1}} = 0$ . Therefore, we only need to prove that the equation

$$1 + x^{2^k-1} + x^{2^{2k-1}-2^{k-1}} = 0 \quad (3)$$

has no solution in  $\mathbb{F}_q$ .

Let  $y = x^{2^k-1}$ . Then computing  $(y * (3))^2$  and simplifying it by  $y^{2^k+1} = 1$ , we get

$$y + y^2 + y^4 = 0. \quad (4)$$

It follows from Lemma 2.5 that (4) has no nonzero solution in  $\mathbb{F}_q$  when  $k \not\equiv 0 \pmod{3}$ . Since  $x = 0$  is not the solution of (3),  $f(x) = 0$  has only one solution in  $\mathbb{F}_q$  when  $k \not\equiv 0 \pmod{3}$ .

Then we prove that  $f(x) = a$  has at most one solution in  $\mathbb{F}_q$  for any  $a \in \mathbb{F}_q^*$  if and only if  $k \not\equiv 0 \pmod{3}$ . Let  $d = 2^{2k-1} - 2^{k-1} + 1$ . Let  $s$  be an integer satisfying  $1 \leq s \leq 2^{2k} - 2$  and  $4s \equiv 2^k + 3 \pmod{2^{2k} - 1}$ . Then it is easy to verify that  $ds \equiv 1 \pmod{2^{2k} - 1}$ . And we have the following equation from  $f(x) = a$ :

$$x + x^{2^k} + x^d = a. \quad (5)$$



Let  $u = x^d + a = x + x^{2^k}$ . Then  $u \in \mathbb{F}_{2^k}$  and  $x = (a + u)^s$ . Plugging it into (5), we have

$$(a + u)^s + (a + u)^{2^k \cdot s} = u.$$

Raising the above equation to the 4-th power and simplifying it, we get

$$u^4 + (a^{2^{k+1}} + a^2)u^2 + (a^{2^k} + a)^3u + a^{2^k+1}(a^2 + a^{2^{k+1}}) = 0. \quad (6)$$

Let  $b = a^{2^k} + a$ ,  $c = a^{2^k+1}$ . Then  $b, c \in \mathbb{F}_{2^k}$ , and the above equation reduces to

$$u^4 + b^2u^2 + b^3u + b^2c = 0.$$

If  $b = 0$ , then there is only one solution  $u = 0$  of the above equation. Hence,  $f(x) = a$  has at most one solution  $x = a^s$  in  $\mathbb{F}_q$  for any  $a \in \mathbb{F}_q^*$ .

If  $b \neq 0$ , let  $u = bv$ . Rewriting the above equation, we get

$$v^4 + v^2 + v = \frac{c}{b^2} = \frac{a^{2^k+1}}{(a^{2^k} + a)^2}. \quad (7)$$

Since  $x = (a + u)^s = (a + bv)^s$ , it suffices to prove that (7) has at most one solution in  $\mathbb{F}_{2^k}$  for any  $a \in \mathbb{F}_q^*$  if and only if  $k \not\equiv 0 \pmod{3}$ . Then the result follows from Lemma 2.5.

We finish the proof. ■

**Theorem 4.8.** *Let  $q = 2^{2^k}$  and  $k > 0$  be an odd integer. Then  $f(x) = x + x^{2^k+2} + x^{2^{2^k-1}+2^{k-1}+1}$  is a permutation trinomial over  $\mathbb{F}_q$ .*

*Proof:* First of all, we show that  $x = 0$  is the only solution of  $f(x) = 0$  in  $\mathbb{F}_q$ . If  $f(x) = 0$ , then either  $x = 0$  or  $1 + x^{2^k+1} + x^{2^{2^k-1}+2^{k-1}} = 0$ . Therefore, we only need to prove the equation

$$1 + x^{2^k+1} + x^{2^{2^k-1}+2^{k-1}} = 0 \quad (8)$$

has no solution in  $\mathbb{F}_q$ . Raising (8) to its 2-th power, we have

$$1 + x^{2^{k+1}+2} + x^{2^k+1} = 0.$$

Let  $y = x^{2^k+1}$ . Then  $y \in \mathbb{F}_{2^k}$ , and we get

$$1 + y + y^2 = 0. \quad (9)$$

It is clear that  $y = 1$  is not the solution of (9). Then multiplying  $(1 + y)$  to both sides, we have  $y^3 = 1$ . We know  $\gcd(2^k - 1, 3) = 1$  since  $k$  is odd. Therefore the above equation has no solution in  $\mathbb{F}_{2^k}$ . Hence,  $x = 0$  is the only solution of  $f(x) = 0$  in  $\mathbb{F}_q$ .

Next, we prove that  $f(x) = a$  has at most one solution in  $\mathbb{F}_q$  for any  $a \in \mathbb{F}_q^*$ . Considering the following equation:

$$1 + x^{2^k+1} + x^{2^{2^k-1}+2^{k-1}} = \frac{a}{x}. \quad (10)$$

Let  $u = \frac{a}{x}$ . Then  $u = 1 + x^{2^k+1} + x^{2^{2k-1}+2^{k-1}} \in \mathbb{F}_{2^k}^*$ . Plugging  $x = \frac{a}{u}$  into the square of (10), we have

$$1 + \frac{a^{2^{k+1}+2}}{u^4} + \frac{a^{2^k+1}}{u^2} = u^2. \quad (11)$$

Let  $y = \frac{a^{2^k+1}}{u^2}$ . Then  $y \in \mathbb{F}_{2^k}$ . Plugging it into (11), we have  $y^3 + y^2 + y = a^{2^k+1}$ .

Since  $g(y) = y^3 + y^2 + y = (y+1)^3 + 1$  is a permutation polynomial over  $\mathbb{F}_{2^k}$  when  $k > 0$  is odd, we know that  $f(x) = a$  has at most one solution in  $\mathbb{F}_q$  for any  $a \in \mathbb{F}_q^*$ . Hence the proof is complete.  $\blacksquare$

Next we introduce three new classes of permutation trinomials with the form  $f(x) = x + ax^\alpha + bx^\beta \in \mathbb{F}_{2^m}[x]$ , where  $a, b \in \mathbb{F}_{2^m}^*$ .

**Theorem 4.9.** *Let  $q = 2^{2k}$  and  $k > 0$  be an integer,  $f(x) = x + ax^{2^{k+1}-1} + a^{2^{k-1}}x^{2^{2k}-2^k+1}$ , where  $a \in \mathbb{F}_q$  and the order of  $a$  is  $2^k + 1$ . Then  $f(x)$  is a permutation trinomial over  $\mathbb{F}_q$ .*

*Proof:* First of all, we show that  $x = 0$  is the only solution to  $f(x) = 0$ . If  $f(x) = 0$ , then either  $x = 0$  or  $1 + ax^{2^{k+1}-2} + a^{2^{k-1}}x^{2^{2k}-2^k} = 0$ . Therefore, we only need to prove the equation

$$1 + ax^{2^{k+1}-2} + a^{2^{k-1}}x^{2^{2k}-2^k} = 0. \quad (12)$$

has no solution in  $\mathbb{F}_q$ . Adding (12) to (12) $^{2^{k+1}}$ , we have

$$x^{3 \cdot 2^k - 3} = a^{3 \cdot 2^{k-1}}.$$

Therefore,  $x^{2^k-1} = a^{2^{k-1}}$  or  $x^{2^k-1} = a^{2^{k-1}}\omega$ , where  $\omega^2 + \omega + 1 = 0$ .

If  $x^{2^k-1} = a^{2^{k-1}}$ , then by plugging it into (12), one get  $1 + a^{2^k+1} + a^{2^{2k-1}+2^{k-1}} = 0$ . Recalling the order of  $a$  is  $2^k + 1$ , we have  $1 = 0$ . It is a contradiction.

If  $x^{2^k-1} = a^{2^{k-1}}\omega$ , then by plugging it into (12), one have  $\omega^{2^k} + \omega^2 + 1 = 0$ . Hence  $\omega^{2^k} = \omega$ , which means that  $k$  is even. However, in this case,  $(a^{2^{k-1}}\omega)^{2^{k+1}} = \omega^{2^k+1} = \omega^2 \neq 1$ . It then follows that the equation  $x^{2^k-1} = a^{2^{k-1}}\omega$  has no solution in  $\mathbb{F}_q$ . Contradicts!

Hence,  $x = 0$  is the only solution to  $f(x) = 0$  in  $\mathbb{F}_q$ .

Next we prove that  $f(x) = c$  has at most one solution in  $\mathbb{F}_q$  for any  $c \in \mathbb{F}_q^*$ . Considering the equation

$$x + ax^{2^{k+1}-1} + a^{2^{k-1}}x^{2^{2k}-2^k} = c.$$

Raising the above equation to the 2-th power, we have

$$x^2 + a^2x^{2^{k+2}-2} + a^{2^k}x^{4-2^{k+1}} = c^2. \quad (13)$$

Computing (13) + (13) $^{2^k} * a$ , and simplifying it by using  $a^{2^k+1} = 1$ , we have

$$x^2 + ax^{2^{k+1}} = c^2 + ac^{2^{k+1}}.$$

Let  $u = x^2 + c^2$ . Then  $u = au^{2^k}$ . Plugging  $x^2 = u + c^2$  into (13), we get

$$u + a^2(u + c^2)^{2^{k+1}-1} + a^{2^k}(u + c^2)^{2-2^k} = 0. \quad (14)$$

Multiplying  $(u + c^2)^{2^k+1}$  across both sides of the above equation and then substituting  $u^{2^k} = u/a$  and  $a^{2^k+1} = 1$  into it, one can get the following equation after simplification.

$$u^3 + \alpha u + \beta = 0, \quad (15)$$

where  $\alpha = ac^{2^{k+1}+2} + c^4 + a^2c^{2^{k+2}}$ ,  $\beta = a^3c^{3 \cdot 2^{k+1}} + c^6$ .

Now let  $\gamma = ac^{2^{k+1}} + c^2$ . Then  $\beta = \gamma\alpha$ . We distinguish two cases.

**Case  $\gamma = 0$ .**

Then  $\alpha = c^4$  and  $\beta = 0$ . Therefore, the solutions of (15) are  $u = 0$  or  $u = c^2$ . So  $x = 0$  and  $x = c$  may be the solutions of the equation  $f(x) = c$ . However,  $f(0) \neq c$ . Hence, in this case,  $f(x) = c$  has one unique nonzero solution  $x = c$  for each nonzero  $c \in \mathbb{F}_q$ .

**Case  $\gamma \neq 0$ .**

If  $\alpha = 0$ , then  $u = 0$  is the only solution of (15).

If  $\alpha \neq 0$ , then let  $u = \alpha^{1/2}\varepsilon$ . Further,  $\alpha^{2^k} = \frac{\alpha}{a^2}$ ,  $\varepsilon^{2^k} = \frac{u^{2^k}}{(\alpha^{1/2})^{2^k}} = \frac{u}{a} \frac{a}{\alpha^{1/2}} = \varepsilon$ . Therefore  $\varepsilon \in \mathbb{F}_{2^k}$ . Dividing (15) by  $\alpha^{\frac{3}{2}}$  results in

$$\varepsilon^3 + \varepsilon + \frac{\gamma}{\alpha^{1/2}} = 0.$$

It is routine to verify that  $\frac{\gamma}{\alpha^{1/2}} \in \mathbb{F}_{2^k}$ . Hence  $h(\varepsilon) = \varepsilon^3 + \varepsilon + \frac{\gamma}{\alpha^{1/2}} \in \mathbb{F}_{2^k}[\varepsilon]$ . According to Lemma 2.6,  $h(\varepsilon) = 0$  has only one solution in  $\mathbb{F}_{2^k}$  if and only if  $\text{Tr}_k\left(\frac{\alpha}{\gamma^2}\right) = \text{Tr}_k(1) + 1$ .

Next, we show that  $\text{Tr}_k\left(\frac{\alpha}{\gamma^2}\right) = \text{Tr}_k(1) + 1$ . We know

$$\begin{aligned} \text{Tr}_k\left(\frac{\alpha}{\gamma^2}\right) &= \text{Tr}_k\left(\frac{ac^{2^{k+1}+2} + c^4 + a^2c^{2^{k+2}}}{c^4 + a^2c^{2^{k+2}}}\right) \\ &= \text{Tr}_k\left(\frac{ac^{2^{k+1}+2}}{c^4 + a^2c^{2^{k+2}}} + 1\right) \\ &= \text{Tr}_k(1) + \text{Tr}_k\left(\frac{ac^{2^{k+1}+2}}{c^4 + a^2c^{2^{k+2}}}\right) \end{aligned}$$

and

$$\text{Tr}_k\left(\frac{ac^{2^{k+1}+2}}{c^4 + a^2c^{2^{k+2}}}\right) = \text{Tr}_k\left(\frac{ac^{2^{k+1}-2}}{1 + a^2c^{2^{k+2}-4}}\right) = \text{Tr}_k\left(\frac{1}{1 + ac^{2^{k+1}-2}} + \frac{1}{(1 + ac^{2^{k+1}-2})^2}\right).$$

Let  $v = \frac{1}{1 + ac^{2^{k+1}-2}}$ . Then  $v^{2^k} = \frac{1}{1 + a^{2^k}c^{2^2-2^{k+1}}} = v + 1$ . Therefore we have

$$\text{Tr}_k\left(\frac{ac^{2^{k+1}+2}}{c^4 + a^2c^{2^{k+2}}}\right) = \text{Tr}_k(v + v^2) = v + v^{2^k} = 1.$$

Hence,  $\text{Tr}_k\left(\frac{\alpha}{\gamma^2}\right) = \text{Tr}_k(1) + 1$ .

Then,  $\text{Tr}_k\left(\frac{\alpha^{1/2}}{\gamma}\right) = \left(\text{Tr}_k\left(\frac{\alpha}{\gamma^2}\right)\right)^{\frac{1}{2}} \neq \text{Tr}_k(1)$ . Hence,  $h(\varepsilon) = 0$  has only one solution in  $\mathbb{F}_{2^k}$  according to Lemma 2.6. Therefore  $f(x) = c$  has at most one solution in  $\mathbb{F}_q$  for any  $c \in \mathbb{F}_q^*$ .

The proof is complete.  $\blacksquare$

**Theorem 4.10.** *Let  $q = 2^{2k+1}$  and  $k > 0$  be an integer. Then  $f(x) = x + ax^{2^{k+1}-1} + a^{2^{2k+1}-2^{k+1}-2}x^{2^{k+1}+1}$ , where  $a \in \mathbb{F}_q$ , is a permutation trinomial over  $\mathbb{F}_q$ .*

*Proof:* The case  $a = 0$  is trivial. Therefore, we assume  $a \neq 0$  in the following.

First of all, we show that  $x = 0$  is the only solution of  $f(x) = 0$  in  $\mathbb{F}_q$ . If  $f(x) = 0$ , then either  $x = 0$  or  $1 + ax^{2^{k+1}-2} + a^{-2^{k+1}-1}x^{2^{k+1}} = 0$ . Therefore, we only need to prove the equation

$$1 + ax^{2^{k+1}-2} + a^{-2^{k+1}-1}x^{2^{k+1}} = 0 \quad (16)$$

has no solution in  $\mathbb{F}_q$ . Raising (16) to the  $2^k$ -th power, we have

$$1 + a^{2^k}x^{1-2^{k+1}} + a^{-2^k-1}x = 0. \quad (17)$$

Multiplying  $a^{2^k+1}x^{2^{k+1}}$  across both sides of (17), we have

$$(x + a^{2^k+1})^{2^{k+1}+1} = a^{2^{k+1}+2^{k+2}}. \quad (18)$$

It is clear that  $\gcd(2^{k+1} + 1, 2^{2k+1} - 1) = 1$ . Hence  $x = 0$  is the only solution of (18) in  $\mathbb{F}_q$ . However, it is not the solution of (16). Hence, (16) has no solution in  $\mathbb{F}_q$ .

Then we prove that  $f(x) = c$  has at most one solution in  $\mathbb{F}_q$  for any  $c \in \mathbb{F}_q^*$ . Considering the following equation:

$$x + ax^{2^{k+1}-1} + a^{-2^{k+1}-1}x^{2^{k+1}+1} + c = 0. \quad (19)$$

Computing  $a^{2^k} * (19) + x^{2^k} * (19)^{2^k}$ , we have

$$a^{2^k+1}x^{2^{k+1}-1} + x^{2^{k+1}} + c^{2^k}x^{2^k} + a^{2^k}c = 0. \quad (20)$$

Then by computing  $(c + x)x^{2^{k+1}-1} * (20)^{2^{k+1}} + a^{2^{k+1}+1}x * (19)$  and after simplification, we get

$$(a^{2^{k+1}+2} + ac^{2^{k+1}} + c^2)x = ac^{2^{k+1}+1}. \quad (21)$$

Since  $a, c \in \mathbb{F}_q^*$ , we know that (21) has at most one solution in  $\mathbb{F}_q$ . Then  $f(x) = c$  has at most one solution in  $\mathbb{F}_q$  for any  $c \in \mathbb{F}_q^*$ . We are done.  $\blacksquare$

Let  $a = 1$  in the above theorem. Then  $f(x) = x + x^{2^{k+1}-1} + x^{2^{k+1}+1}$  and  $f(x^{2^{k+1}+2}) = x^{2^{k+1}} + x^{2^{k+1}+2} + x^{3 \cdot 2^{k+1}+4}$ , which is the permutation trinomial in Theorem 4.1(6). Hence Theorem 4.10 is a generalization of a known permutation trinomial.

A comment about Theorem 4.10 is as follows. Just after our submission, we noticed that this class of permutation trinomial was also introduced in a very recent paper. In [21], Ma et al. presented several classes

of new permutation polynomials, including two classes of permutation trinomials, that is, [21, Theorem 5.1 and Theorem 5.2]. It can be readily verified that Theorem 4.10 is equivalent to [21, Theorem 5.1], though our proof is different and a bit short.

The last class of permutation trinomial is a generalization of the second permutation trinomial in Theorem 4.2 ([9, Theorem 2.2]).

**Theorem 4.11.** *Let  $q = 2^{2k+1}$ ,  $f(x) = x + ax^3 + a^{2^{2k+1}-2^{k+1}}x^{2^{2k+1}-2^{k+2}+2}$ ,  $a \in \mathbb{F}_q$ . Then  $f(x)$  is a permutation trinomial over  $\mathbb{F}_q$ .*

*Proof:* The case  $a = 0$  is trivial. If  $a = 1$ , then it reduces to [9, Theorem 2.2]. Therefore, we assume  $a \neq 0, 1$  in the following.

Let  $y = x^{2^{k+1}}$  and  $b = a^{2^{k+1}}$ . Then  $y^{2^{k+1}} = x^2$  and  $b^{2^{k+1}} = a^2$ . For all  $x \in \mathbb{F}_q^*$ , we have

$$f(x) = x + ax^3 + \frac{a}{b} \frac{x^3}{y^2} = \frac{x(abx^2y^2 + by^2 + ax^2)}{by^2}. \quad (22)$$

First, we show that  $x = 0$  is the only solution of  $f(x) = 0$  in  $\mathbb{F}_q$ . From (22), we only need to prove the equation

$$abx^2y^2 + by^2 + ax^2 = 0 \quad (23)$$

has no solution in  $\mathbb{F}_q^*$ . Raising (23) into its  $2^{k+1}$ -th power, we have

$$ba^2x^4y^2 + a^2x^4 + by^2 = 0. \quad (24)$$

Computing  $(23)^2 + (24)$ , we have

$$(1 + ax^2)^{2^{k+1}+2} = 0.$$

Then  $x^2 = \frac{1}{a}$  and  $y^2 = \frac{1}{b}$ . Plugging them into (23), we get  $1 = 0$ . It is a contradiction.

If  $f(x)$  is not a permutation polynomial of  $\mathbb{F}_q^*$ , then there exists  $x \in \mathbb{F}_q^*$  and  $c \in \mathbb{F}_q^*$  such that  $f(x) = f((1+c)x)$ . Let  $d = c^{2^{k+1}}$ . It is clear that  $c, d \neq 0, 1$  and  $c \neq d$ . Then

$$\frac{x(by^2 + abx^2y^2 + ax^2)}{by^2} = \frac{(1+c)x(b(1+d)^2y^2 + ab(1+c)^2(1+d)^2x^2y^2 + a(1+c)^2x^2)}{b(1+d)^2y^2},$$

After simplifying, we get

$$A_1x^2y^2 + A_2y^2 + A_3x^2 = 0, \quad (25)$$

where

$$\begin{aligned} A_1 &= abc(1+d)^2(c^2 + c + 1), \\ A_2 &= bc(1+d)^2, \\ A_3 &= a[(1+d)^2 + (1+c)^3]. \end{aligned}$$

Raising (25) to  $2^{k+1}$ -th power, we have

$$A_1^{2^{k+1}} x^4 y^2 + A_3^{2^{k+1}} y^2 + A_2^{2^{k+1}} x^4 = 0. \quad (26)$$

Computing  $(25)^*(A_1^{2^{k+1}} x^4 + A_3^{2^{k+1}}) + (26)^*(A_1 x^2 + A_2)$ , we get

$$B_1 x^4 + B_2 x^2 + B_3 = 0. \quad (27)$$

where

$$\begin{aligned} B_1 &= A_3 A_1^{2^{k+1}} + A_1 A_2^{2^{k+1}} = a^3 b d^2 (1+c)^4 [(1+c)^3 + (1+d)^3], \\ B_2 &= A_2^{2^{k+1}+1} = a^2 b c d (1+c)^4 (1+d)^2, \\ B_3 &= A_3^{2^{k+1}+1}. \end{aligned}$$

It is routine to verify that  $A_1, A_2, B_1, B_2 \neq 0$ . Let  $x^2 = \frac{B_2}{B_1} \varepsilon$ . Plugging it into (27), we have

$$\varepsilon^2 + \varepsilon + D = 0, \quad (28)$$

where  $D = \frac{B_1 B_3}{B_2^2}$ . As for  $D$ , we know

$$D = \frac{B_1 B_3}{B_2^2} = \frac{A_3^{2^{k+1}+1} (A_3 A_1^{2^{k+1}} + A_1 A_2^{2^{k+1}})}{A_2^{2^{k+2}+2}} = \frac{A_1 A_3^{2^{k+1}+1}}{A_2^{2^{k+1}+2}} + \frac{A_1^{2^{k+1}} A_3^{2^{k+1}+2}}{A_2^{2^{k+2}+2}} = D_1 + D_1^{2^{k+1}},$$

where

$$D_1 = \frac{A_1 A_3^{2^{k+1}+1}}{A_2^{2^{k+1}+2}} = \frac{A_1 B_3}{A_2 B_2} = \frac{(c^2 + c + 1)[(1+c)^4 + (1+d)^3][(1+d)^2 + (1+c)^3]}{c d (1+d)^2 (1+c)^4}.$$

Now we claim that  $\text{Tr}_{2k+1}(D_1) = 1$ . It is the same claim appeared in the proof of [9, Theorem 2.2]. The proof of this claim is a bit long and intricate. We omit it here. The interested reader please refer [9] for details.

Raising (28) to  $2^i$ -th power, where  $i = 0, 1, \dots, k$ , and summing them, we get

$$\varepsilon^{2^{k+1}} = \varepsilon + \sum_{i=0}^k (D_1 + D_1^{2^{k+1}})^{2^i} = \varepsilon + \sum_{i=0}^{2k+1} D_1^{2^i} = \varepsilon + D_1 + \text{Tr}_{2k+1}(D_1) = \varepsilon + D_1 + 1.$$

and

$$\varepsilon^{2^{k+1}+1} = \varepsilon(\varepsilon + D_1 + 1) = D_1 \varepsilon + D.$$

Substituting  $x^2 = \frac{B_2}{B_1} \varepsilon$ ,  $y^2 = (\frac{B_2}{B_1})^{2^{k+1}} \varepsilon^{2^{k+1}}$  and the above two equations into (25), we obtain

$$\frac{A_1 B_2^{2^{k+1}+1}}{B_1^{2^{k+1}+1}} (D_1 \varepsilon + D) + \frac{A_2 B_2^{2^{k+1}}}{B_1^{2^{k+1}}} (\varepsilon + D_1 + 1) + \frac{A_3 B_2}{B_1} \varepsilon = 0.$$

Multiplying  $B_1^{2^{k+1}+1}$  across the two sides of the above equation and using  $B_2^{2^{k+1}} = A_2^{2^{k+1}+2} = A_2 B_2$ , we

have

$$C_1\varepsilon + C_2 = 0,$$

where

$$\begin{aligned} C_1 &= A_1A_2B_2D_1 + A_2^2B_1 + A_3B_1^{2^{k+1}} = A_1A_2^{2^{k+1}+2}, \\ C_2 &= A_1A_2B_2D + A_2^2B_1(D_1 + 1) = A_2^2B_1. \end{aligned}$$

Therefore,  $\varepsilon = \frac{C_2}{C_1} = \frac{B_1}{A_1A_2^{2^{k+1}}} = \frac{A_2B_1}{A_1B_2}$ . Plugging it into (28), we have

$$B_1A_2^2 + A_1A_2B_2 = A_1^2B_3.$$

That is  $A_1^{2^{k+1}}A_2^2 = A_1^2A_3^{2^{k+1}}$ . Substituting the definitions of  $A_1, A_2, A_3$  into the above equation, we get

$$a^2bd(1+c)^4(d^2+d+1)b^2c^2(1+d)^4 = a^2b^2c^2(1+d)^4(c^2+c+1)^2b[(1+c)^4 + (1+d)^3].$$

Simplifying it, we have  $(1+d)^3 = (1+c)^6$ . Since  $\gcd(3, 2^{2k+1} - 1) = 1$ , one get  $d = c^2$ . After raising it to the  $2^{k+1}$ -th power, we obtain  $c^2 = d^2 = d$ , which means  $d = 0, 1$ . It is a contradiction since  $d \neq 0, 1$ .

Hence, the proof is complete. ■

### C. Multiplicative inequivalence of the new permutation trinomials with known ones

In this subsection, we briefly discuss the multiplicative inequivalence of the new permutation trinomials with known ones.

First, the last three classes of permutation trinomials are not with trivial coefficients. As far as the authors know, there exist only five such classes of permutation trinomials in  $\mathbb{F}_{2^m}$ . They are the functions in Theorem 4.1 (5), (7), (8), Theorems 4.5 and 4.6. Any of our newly constructed permutation trinomial is multiplicative inequivalent to those in Theorem 4.1 (5), (7) since the latter permutations are defined over  $\mathbb{F}_{2^{3k}}$ . The three conditions in Theorem 4.1 (8) are further investigated in [20]. In general, no simple conditions can make  $h(x)$  into a permutation trinomial. Hence it is multiplicative inequivalent to any of our newly constructed permutation trinomial. The permutations in Theorems 4.10, 4.11 are multiplicative inequivalent to those in Theorems 4.5, 4.6 since they are defined over odd dimension, while the latter permutations are defined over even dimension. It can be easily verified that the function in Theorem 4.9 is multiplicative inequivalent to those in Theorems 4.5, 4.6. Hence the permutation trinomials in Theorems 4.9, 4.10 and 4.11 are indeed multiplicative inequivalent to known permutations. Further, they are pairwise multiplicative inequivalent.

In [21], two classes of permutation trinomials were introduced. The first one is equivalent to Theorem 4.10. The second one is as follows.

**Theorem 4.12.** [21, Theorem 5.2] *Let  $m > 1$  be an odd integer such that  $m = 2k - 1$ . Then  $f(x) = x + ux^{2^k-1} + u^{2^k}x^{2^m-2^{k+1}+2}$ ,  $u \in \mathbb{F}_{2^m}$ , is a permutation polynomial over  $\mathbb{F}_{2^m}$ .*

We only need to check the multiplicative equivalence between the permutation trinomials in Theorems 4.11 and 4.12. It can be easily verified that they are indeed multiplicative inequivalent.

Now let us discuss the first two classes of permutation trinomials with trivial coefficients. We need to show they are multiplicative inequivalent to all the known classes. To this end, we used a Magma program to confirm this conclusion for at least one small field  $\mathbb{F}_{2^m}$ , where  $4 \leq m \leq 10$ . Consequently, these two classes of permutation trinomials are also new. Further, these two classes are also multiplicative inequivalent to each other.

## 5. CONCLUSIONS

Permutation binomials and permutation trinomials over finite fields are both interesting and important in theory and in many applications. In this paper, we present several new classes of permutation binomials and permutation trinomials. These functions extend the list of known such permutations. However, from computer experiments, we found that there should be more classes of permutation binomials and permutation trinomials. A complete determination of all permutation binomials or all permutation trinomials over finite fields seems to be out of reach for the time being. The constructed functions here lay a solid foundation for the further research.

At last, we would like to mention that the constructed functions have many applications. For instances, they can be employed in linear codes [4] and cyclic codes [8], they can also be used to construct highly nonlinear functions such as bent and semi-bent functions. For more details, please refer to the last paragraph in [9] and the references therein.

## REFERENCES

- [1] S. Ball, M. Zieve, Symplectic spreads and permutation polynomials, in: Finite Fields and Applications, in: Lect. Notes Comput. Sci., vol.2948, Springer, Berlin, 2004, pp. 79-88.
- [2] E.R.Berlekamp, H.Rumsey, G.Solomon. On the solution of algebraic equations over finite fields[J]. Information And Control, 1967, 10(67), pp. 553-564.
- [3] A. BLOKHUIS, R. S. COULTER, M. HENDERSON AND C. M. O'KEEFE, *Permutations amongst the Dembowski-Ostrom polynomials*, In: D. Jungnickel and H. Niederreiter, Eds., Finite Fields and Applications: Proceedings of the Fifth International Conference on Finite Fields and Applications, 2001, pp. 37-42.
- [4] C. Carlet, C. Zha, J. Yuan, Linear codes from highly nonlinear functions and their secret sharing schemes, IEEE Trans. Inform. Theory, 51(2005), pp. 2089-2102.
- [5] W.Cherowitzo,  $\alpha$ -flocks and hyperovals, Geom. Dedic. 72 (1998), pp. 221-246.
- [6] L.E. Dickson, History of the Thoery of Numbers, vol.3, Carnegie Institute, Washington, D.C., 1923, Dover, New York, 2005.
- [7] L.E. Dickson, The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group, Annals Math. 11 (1896-1897), 65-120 and 161-183.



- [8] C. Ding, Cyclic Codes from some monomials and trinomials, *SIAM J. Discrete Math.*, 27(2013), pp.1977-1994.
- [9] C. Ding, L. Qu ,Q. Wang, et al. Permutation trinomials over finite fields with even characteristic[J]. *SLAM J. Dis. Math*, 29(2015), pp. 79-92.
- [10] H. Dobbertin, Almost perfect nonlinear power functions on  $\mathbf{GF}(2^n)$ : the Welch case, *IEEE Trans.Inf.Theory*, 45 (1999), pp. 1271-1275.
- [11] H. Dobbertin, Uniformly representable permutation polynomials, in *Preceedings of SETA 01*, T.Helleseth, P.V. Kumar, and K. Yang, eds., Springer London, 2002, pp. 1-22.
- [12] Ch. Hermite, Sur les fonctions de sept lettres, *C.R. Acad. Sci. Paris* **57** (1863), pp. 750-757.
- [13] X. Hou, S.D.Lappano, Determination of a type of permutaiton binomials over finite fields, *J.Number Theory*, 147(2015), pp. 14-23.
- [14] X. Hou, A survey of permutation binomials and trinomials over finite fields ,in: G. Kyureghyan, G.L. Mullen, A. Pott (Eds.), *Topics in Finite Fields, Proceedings of the 11th International Conference on Finite Fields and Their Applications*, Contemp. Math., Magdeburg, Germany, July 2013, vol. 632, AMS (2015), pp. 177-191.
- [15] X. Hou, Permutation polynomials over finite fields–A survey of recent advances, *Finite Fields Appl.* 32(2015), pp. 82-119.
- [16] X. Hou, A class of permutation trinomials over finite fields, *Acta Arith.* 162(2014), pp. 51-64.
- [17] X. Hou, Determination of a type of permutaiton trinomials over finite fields, *Acta Arith.* 162(2014), pp. 253-278.
- [18] X. Hou, Determination of a type of permutaiton trinomials over finite fields, **II**, *Finite Fields Appl.* 35(2015), pp. 16-35.
- [19] S.D. Lappano, A note regarding permutation binomials over  $\mathbb{F}_{q^2}$ , *Finite Fields Appl.* 34(2015), pp. 153-160.
- [20] J. B. LEE AND Y. H. PARK, Some permutation trinomials over finite fields, *Acta Math. Sci.*, 17 (1997), pp. 250–254.
- [21] J. Ma, T. Zhang, T. Feng and G. Ge, New results on permutation polynomials over finite fields, <http://arxiv.org/abs/1506.05525v2>.
- [22] R. Lidl, H. Niederreiter, *Finite Fields*, 2nd ed. Cambridge Univ. Press, Cambridge, 1997.
- [23] G.L. Mullen, D. Panario, *Handbook of Finite Fields*, Taylor And Francis. Boca Raton, 2013.
- [24] Z. Tu, X. Zeng, L. Hu, C. Li, A class of binomial permutation polynomials, *arXiv:1310.0337*, 2013.
- [25] Z. TU, X. ZENG, AND L. HU, Several classes of complete permutation polynomials, *Finite Fields and Appl.*, 25 (2014), pp. 182–193.
- [26] B. Wu, Z. Liu, Linearized polynomials over finite fields revisited , *Finite Fields Appl.*, 22 (2013), pp. 79-100.
- [27] M.E. Zieve, On some permutation polynomials over  $\mathbb{F}_q$  of the form  $x^r h(x^{(q-1)/d})$ , *Proc. Am. Math. Soc.* 137 (2009), pp. 2209-2216.

- [28] M.E. Zieve, Permutation polynomials on  $\mathbb{F}_q$  induced from bijective Rédei functions on subgroups of the multiplicative group of  $\mathbb{F}_q$ , arXiv:1310.0776, 2013.